Abstract

Methods and arrangements for virtual private network (VPN) data packets are disclosed. VPN packets include a payload having Internet Protocol (IP) addresses which guide the packet through a network to a security gateway. The payload may be encrypted and/or compressed and may include internal addresses to denote the real source and destination for a data portion of the payload. The destination security gateway for a packet includes a plurality of protocol modules, each for performing a different VPN protocol and a discriminator. As packets are received by the gateway, the discriminator responds to packet addressing information to selectively gate the packet to one or more protocol modules to gain access to the payload. ~~As initial control packets are received they are authenticated and rules and procedures are identified for proper treatment of VPN data packets bearing the same source IP address. The rules and procedures are stored in a gateway data engine having a plurality of protocol processing modules. VPN data packets are received by a protocol discriminator which reads the stored rules and procedures identified for the source IP address of the received packet. The discriminator passes the received packet to a first protocol module as identified in the stored rules and procedures. After the first module completes processing, the packet is passed back to the protocol discriminator which determines whether further protocol processing is required. When further protocol processing is required, the packet is passed to another protocol module for processing in accordance with another protocol. At the completion of processing, the second protocol module returns the packet to the protocol discriminator.~~